UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/465,629	12/17/1999	LEWIS T. DONZIS	NORT-0030-US	9110

7590   10/17/2003

DAN C HU
TROP PRUNER HU & MILES PC
8554 KATY FREEWAY
SUITE 100
HOUSTON, TX 77024

EXAMINER
WU, ALLEN S

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 10/17/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

-- The MAILING DATE of this communication appears on the cover sheet with the correspond nc address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☐ Responsive to communication(s) filed on _____ .

2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) _1-34_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) _1-34_ is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☒ The drawing(s) filed on _17 December 1999_ is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.

    If approved, corrected drawings are required in reply to this Office action.

12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

    a) ☐ The translation of the foreign language provisional application has been received.

15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____ .

DETAILED ACTION

Specification

1.   The title of the invention is not descriptive. A new title is required that is

clearly indicative of the invention to which the claims are directed.

The following title is suggested: Routing Data to One or More Entities in a

Network Using Network Address Translation.

Claim Rejections - 35 USC § 102

1.   The following is a quotation of the appropriate paragraphs of 35

U.S.C. 102 that form the basis for the rejections under this section made in this

Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

2.   Claims 1-7 and 9-34 are rejected under 35 U.S.C. 102(a) as being

anticipated by Nessett et al, US Patent 6,055,236.

As per claim 1, Nessett et al discloses a method of routing

(Abstract) a data unit (data packets, col 7 ln 8-33) targeted to one of a

plurality of entities in a network (multiple network devices, col 7 ln 8-33),

comprising: receiving the data unit (IP packet arrives at the router, col 32

ln 50-64), the data unit including security information (AH or ESP IPsec

packet, col 32 ln 50-64; locally unique security values, col 27 ln 36-50) and

address information (network address for first network device, col 27 ln

36-50; global IP address placed in service request packet, col 35 ln 64-67

and col 36 ln 1-12); and translating the address information to an address

of a target network entity based on the security information (using SPI's to

determine a local IP address, col 32 ln 50-64).

As per claim 2, Nessett et al discloses the address information, in

the data unit, including a common address associated with the plurality of

network entities (global IP address placed in service request packet, col

35 ln 64-67 and col 36 ln 1-12), and each network entity is assigned a

unique network address (local IP address, col 32, ln 50-64), and wherein

translating the address information includes translating the common

address to one of the unique network addresses (using SPI's to determine

a local IP address, col 32 ln 50-64; translate external network address to

internal network address, col 8 ln 30-40).

As per claim 3, Nessett et al discloses receiving an Internet

Protocol packet (IPsec header protocols are added to a IP packet, col 21

ln 43-47).

As per claim 4, Nessett et al discloses translating an Internet

Protocol destination address (determine local IP address of a destination

network device, col 32 ln 50-64).

As per claim 5, Nessett et al discloses receiving a packet including Encapsulating Security Payload information (IPsec header protocols are added to a IP packet...security services are an Authentication Header or a Encapsulating Security Payload header, col 21 ln 43-57).

As per claim 6, Nessett et al discloses translating the address information based on a Security Parameters Index field of the Encapsulating Security Payload information (using SPI's to determine a local IP address, col 32 ln 50-64; IPsec is well known in the art to define two security services. One of them being Encapsulating Security Payload. The Security Parameters Index of the IPsec can be referring to any security service defined by IPsec. Therefore, Security Parameters index of Encapsulating Security Payload information is to be inherent to the teachings of Nessett et al.).

As per claim 7, Nessett et al discloses receiving a packet including Internet Security Association and Key Management Protocol information (Internet Security Association and Key Exchange Protocol to establish security association col 25 ln 1-25; Nessett et al does not explicitly teach Internet Security Association and Key Management Protocol (hereinafter referred to as ISAKMP) information in the data unit. ISAKMP is a standard protocol that is well known in the art. When ISAKMP is being used to establish a Security Association, its header is placed with the IP

packet. Therefore, the data unit containing IP address information

inherently contains ISAKMP information in the teachings of Nessett et al).

As per claim 9, Nessett et al discloses creating one or more

address translation tables (SPI-to-internal-network address table, col 27 ln

51-67 and col 28 ln 1-34) used in the translation of address information

(col 27 51-67 and col 28 ln 1-34), the one or more address translation

tables each containing the address of at least one of the network entities

and security information associated with the at least one network entity

(local IP address for first network device is stored with the one or more

locally unique SPI values in a table, col 27 51-67 and col 28 ln 1-34).

As per claim 10, Nessett et al discloses matching the security

information in the data unit with the information in the one or more address

translation tables (table is used to maintain a mapping between a network

device and a locally unique SPI, col 28 ln 1-34).

As per claim 11, Nessett et al discloses a router for use in a

network having one or more entities (col 7 ln 8-33), the router comprising:

an interface adapted to receive a data unit (col 7 ln 8-33); It is noted that

Nessett et al does not explicitly state an interface adapted to receive a

data unit. However, in order for a router to receive and process IP

packets, an interface in the router is necessary. Therefore, an interface adapted to receive a data unit is inherent to the invention of Nessett et al)

Nessett et al further discloses the data unit containing a field having security information (AH or ESP IPsec packet, col 32 ln 50-64; locally unique security values, col 27 ln 36-50); and a translator adapted to generate an identifier of a network entity that the data unit is targeted for (Network Address Translation router, col 8 ln 30-52) based on the security information (using SPI's to determine a local IP address, col 32 ln 50-64).

As per claim 12, Nessett et al discloses a many-to-one network address translator (Network address translator router, col 8 ln 30-40; It is noted that Nessett et al does not explicitly state a many-to-one network address translator. The translator disclosed by Nessett et al translates local IP addresses of network entities to one common, external, address. Therefore, the translator of Nessett et al is inherently a many-to-one address translator).

As per claim 13, Nessett et al discloses the data unit further contains an address associated with the router (external common network address, col 7 ln 8-33; The common address being associated with the router is to be inherent to the invention of Nessett et al. The global external IP address needs to be associated with a router in order for other

external networks, such as the Internet, to communicate with the internal

network through the router)

As per claim 14, Nessett et al discloses the translator being

adapted to further replace the address with the identifier of the target

network entity (map destination port to internal IP address, col 16 ln 13-25;

using SPI's to determine a local IP address, col 32 ln 50-64).

As per claim 15, Nessett et al discloses translating an Internet

Protocol destination address (determine local IP address of a destination

network device, col 32 ln 50-64).

As per claim 16, Nessett et al discloses a Security Parameters

Index field of the Encapsulating Security Payload information (using SPI's

to determine a local IP address, col 32 ln 50-64; IPsec is well known to

define two security services. One of them being Encapsulating Security

Payload. The Security Parameters index of the IPsec can be referring to

any security service defined by IPsec. Therefore Security Parameters

index of Encapsulating Security Payload information is to be inherent to

the teachings of Nessett et al.).

As per claim 17, Nessett et al discloses the data unit containing

initiator and responder cookies in an Internet Security Association and Key

Management Protocol (here in after referred to as ISAKMP) header (using

ISAMKP for Security Association negotiation, col 25 ln 16-25; Nessett et al

does not explicitly teach initiator and responder cookies in the data unit.

ISAKMP is a standard protocol that is well known in the art. When

ISAKMP is being used to establish a Security Association, its header is

placed with the IP packet. The header information includes initiator and

responder cookies. Therefore, the data unit containing initiator and

responder cookies in an ISAKMP is to be inherent to the teachings of

Nessett et al.)

As per claim 18, Nessett et al discloses a storage medium storing

one or more tables containing routing information accessible by the

translator (SPI-to-internal-network address table, col 27 ln 51-67 and col

28 ln 1-34).

As per claim 19, Nessett et al discloses the routing information

includes security information and a corresponding identifier of a network

entity (local IP address for first network device is stored with the one or

more locally unique SPI values in a table, col 27 51-67 and col 28 ln 1-34).

As per claim 20, Nessett et al discloses an article including one or

more machine-readable storage media containing instructions for routing

(col 8 ln 8-19) a data unit targeted to an entity on a network (col 7 ln 8-33),

the instructions when executed causing a system to: receive the data unit

(IP packet arrives at the router, col 32 ln 50-64), the data unit containing

security information to provide secure communications of the data unit

(AH or ESP IPsec packet, col 32 ln 50-64; locally unique security values,

col 27 ln 36-50); and determine an address of the network entity based on

the security information (using SPI's to determine a local IP address, col

32 ln 50-64).

As per claim 21, Nessett et al discloses translating an address in

the data unit to the address of the network entity based on the security

information (using SPI's to determine a local IP address, col 32 ln 50-64;

translating an external network address to an internal network address for

incoming traffic, col 8 ln 30-40l).

As per claim 22, Nessett et al discloses translating the address

based on Encapsulating Payload Security information (using SPI's to

determine a local IP address, col 32 ln 50-64; IPsec is well known to

define two security services. One of them being Encapsulating Security

Payload. The Security Parameters index of the IPsec can be referring to

any security service defined by IPsec. Therefore Encapsulating Security

Payload information is to be inherent to the teachings of Nessett et al.).

As per claim 23, Nessett et al discloses translating the address

based on Internet Security Association and Key Management Protocol

information (ISAMKP and IKE for SA negotiation, col 26 ln 1-25).

As per claim 24, Nessett et al discloses accessing an address

translation table to match the security information in the data unit to

information in the address translation table (table is used to maintain a

mapping between a network device and a locally unique SPI, col 28 ln 1-

34).

As per claim 25, Nessett et al discloses matching address and

security information in the data unit with address and security information

in the address translation table (SPI-to-internal network address table, col

27 ln 36-67; table is used to maintain a mapping between a network

device and a locally unique SPI, col 28 ln 1-34).

As per claim 26, Nessett et al discloses a data signal embodied in a

carrier wave (electric signal, col 8 ln 8-19) comprising one or more code

segments containing instructions (data bits, col 8 ln 8-19) for routing a

data unit to one of a plurality of network entities (col 7 ln 8-33), the

instructions when executed causing a system to: receive the data unit

having security information and a destination address (IP packet arrives at

the router, col 32 ln 50-64); access one or more translation tables (SPI-to-

internal-network address table, col 27 ln 51-67 and col 28 ln 1-34) each

containing security information and an address of a network entity (local IP

address for first network device is stored with the one or more locally

unique SPI values in a table, col 27 51-67 and col 28 ln 1-34); and convert

the destination address of the data unit to the network entity address

(determine local IP address, col 27 51-67 and col 28 ln 1-34).

As per claim 27, Nessett et al discloses a data unit containing a first

destination address (external network address, col 8 ln 30-40) and the

network entity having a second address (internal network address, col 8 ln

30-40), the data structure (IP packet col 32 ln 50-64) comprising the first

destination address (external network address, col 8 ln 30-40), the second

address (internal network address, col 8 ln 30-40), and security

information (Security Parameter Index, col 21 ln 57-67) useable by the

system to match the first destination address to the second address based

on the security information (using SPI's to determine a local IP address,

col 32 ln 50-64).

As per claim 28, Nessett et al discloses a communications network

(network system, col 7 ln 8-33, comprising: a first network including a

plurality of entities and a router (network devices and router, col 7 ln 8-33),

the router including a network address translator (network address

translation router, col 8 ln 39-40); and a node capable of communicating

data units with entities in the first network (internet or intranet, col 7 ln 34-

49), each data unit including security information (AH or ESP IPsec

packet, col 32 ln 50-64; locally unique security values, col 27 ln 36-50), the

network address translator adapted to convert a destination address in a

received data unit from the node to an address of one of the entities

(translates an external network address to an internal network address,

col 8 ln 30-40) based on the security information in the received data unit

(using SPI's to determine a local IP address, col 32 ln 50-64).

As per claim 29, Nessett et al discloses a system (network system,

col 7 ln 8-33) for use in a network having a plurality of entities (network

devices, col 7 ln 8-33), the system comprising: means for communicating

data units originated by and destined for the plurality of network entities

(route data packets, col 7 ln 8-33); and means for creating information

accessible for routing data units (IP packet, col 32 ln 50-64) the

information containing addresses of the network entities (network address

for first network device, col 27 ln 36-50; global IP address placed in

service request packet, col 35 ln 64-67 and col 36 ln 1-12); and

corresponding security information (AH or ESP IPsec packet, col 32 ln 50-

64; locally unique security values, col 27 ln 36-50).

As per claim 30, Nessett et al discloses means for accessing the

created information to perform routing of the data units based on security

information contained in the data units (using SPI's to determine a local IP address, col 32 ln 50-64).

As per claim 31, Nessett et al discloses accessing means includes a network address translator (Network address translator router, col 8 ln 30-40).

As per claim 32, Nessett et al discloses matching address (internal and external address, col 8 ln 30-40) and security information in the data units (AH or ESP IPsec packet, col 32 ln 50-64; locally unique security values, col 27 ln 36-50) to corresponding address and security information in the created information (SPI-to-internal network address table... maintain a mapping between a network device and a locally unique SPI, col 27 ln 36-67 and col 28 ln 1-9).

As per claim 33, Nessett et al discloses security information including Encapsulating Security Payload information (using SPI's to determine a local IP address, col 32 ln 50-64; IPsec is well known to define two security services. One of them being Encapsulating Security Payload. The Security Parameters index of the IPsec can be referring to any security service defined by IPsec. Therefore Encapsulating Security Payload information is to be inherent to the teachings of Nessett et al).

As per claim 34, Nessett et al discloses the security information

including Internet Security Association and Key Management Protocol

information (Internet Security Association and Key Exchange Protocol to

establish security association col 25 ln 1-25; Nessett et al does not

explicitly teach Internet Security Association and Key Management

Protocol (hereinafter referred to as ISAKMP) information in the packet.

ISAKMP is a standard protocol that is well known in the art. When

ISAKMP is being used to establish a Security Association, its header is

placed with the IP packet.   Therefore, the data unit in the teachings of

Nessett et al inherently contains ISAKMP information).

Claim Rejections - 35 USC § 103

3.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for

all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described
> as set forth in section 102 of this title, if the differences between the subject matter sought to
> be patented and the prior art are such that the subject matter as a whole would have been
> obvious at the time the invention was made to a person having ordinary skill in the art to which
> said subject matter pertains. Patentability shall not be negatived by the manner in which the
> invention was made.

4.   Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over

Nessett et al, US Patent 6,055,236, in view of Maughan et al.

As per claim 8, Nessett et al discloses translating the address

information based on a Security Parameters Index (using SPI's to

determine a local IP address, col 32 ln 50-64). Furthermore, Nessett et al

discloses security information including Internet Security Association and

Key Management Protocol (herein after referred to as ISAKMP) (Internet

Security Association and Key Exchange Protocol to establish security

association col 25 ln 1-25; Nessett et al does not explicitly teach Internet

Security Association and Key Management Protocol (hereinafter referred

to as ISAKMP) information in the packet. (ISAKMP is a standard protocol

that is well known in the art. When ISAKMP is being used to establish a

Security Association, its header is placed with the IP packet.   Therefore,

the data unit in the teachings of Nessett et al inherently contains ISAKMP

information).

Nessett et al does not teach translating the address based on

initiator and responder cookies of the ISAKMP. Maughan et al discloses

Internet Security Association and Key Management Protocol with a header

including initiator and responder cookies (page 21). The initiator and

responder cookies correspond to information identifying the initiator and

responder devices. The Security Parameters Index field of Encapsulating

Security Payload information also identifies the network entities for a

Security Association. Both the cookies and the Security Payload Index

field serve as some kind of identification of network entities requesting the

Security Association and are stored as digital data in the headers of the

corresponding protocol. It would have been obvious to one of ordinary

skill at the time of the applicant's invention to combine the teachings of

Maughan et al within the system of Nessett et al because it would have

provided another security protocol for identifying and translating network

addresses information to a local network entity.

Conclusion

5.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure.

Holden et al, US Patent 6,067,620, discloses routing data packets

according to user's security information.

Mayes et al, US Patent 5,793,763, discloses translating local IP addresses

to globally unique IP addresses.

Borella et al, US Patent 6,353,614, discloses a method and protocol for

distributed network address translation.

Boden et al, US Patent, 6,615,357, discloses network address translation

in a virtual private network.

Any inquiry concerning this communication or earlier communications from

the examiner should be directed to Allen S. Wu whose telephone number is 703-

305-0708. The examiner can normally be reached on Monday-Friday 9am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the

examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax

phone number for the organization where this application or proceeding is

assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application

or proceeding should be directed to the receptionist whose telephone number is

703-305-0900.

Allen S. Wu
Examiner
Art Unit 2131

ASW

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOG'. CENTER 2100